DETAILED ACTION

This action is in response to the Amendment filed 3/17/2009.

Response to Arguments

Applicant's arguments with respect to claims have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-3, 5, 6, 8-10, 14, 15, 19-25 and 28-39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ji et al (5,623,600) in view of Nachenberg (U.S. 5,696,822).

Ji teaches with respect to claim 1, a method comprising: receiving computer data (files) from a first computer (i.e. a node from which files came) at a intermediary computer (see figure 1 element 33 gateway node); screening (figure 8B) the computer data for at least one virus using the intermediary to produce a screening result (see Ji Abstract, column 3 lines 52-63 and column 10 lines 26 – column 11 line 40); and communicating the screening result from the intermediary to the second computer

(column 10 lines 26 – column 11 line 40 i.e. a recipient node which is to receive the files)

Ji does not teach wherein the intermediary computer is a model of the second computer and receiving at a model of a second computer a status update communication from the second computer the status update communication including pre-existing information on the second computer; updating and maintaining the model based on the status update communication to reflect any changes to the second computer.

Nachenberg teaches wherein the intermediary computer is a model of the second computer (Virtual machine) and receiving at a model of a second computer a status update communication from the second computer the status update communication including pre-existing information on the second computer; updating and maintaining the model based on the status update communication to reflect any changes to the second computer (see Nachenberg figure 4A and column 10 lines 12-57).

It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have install the computer data on a model machine to check of virus because it is the safest and most reliable way of check for viruses (see column 1 lines 34-46). Therefore one would have been motivated to have installed computer data on a model machine for the scanning of viruses.

With respect to claim 2, wherein the network comprises an IP network for transmission of the computer data and the screening result (see Ji column 4 lines 17-32).

With respect to claim 3, if the at least one virus is detected, performing at least one of the following: (i) inhibiting communication of at least a portion of the computer data to the second computer; (ii) removing the at least one virus from the computer data prior to transferring the computer data to the second computer; (iii) communicating a message indicating that the at least one virus was detected to the second computer; (iv) communicating a message indicating that the at least one virus was detected to the first computer; and (v) writing data to a database indicating that the at least one virus was detected (see Ji figures 8A, 8B, 8C and column 11 lines 6-40).

With respect to claim 5, a virus screening system operative to be connected to a network and operative to screen computer data for at least one virus when the computer data is transmitted between a first compute (e.g. an element 30 in network 22) and a second computer (e.g. an element 30 in network 24), the virus screening device comprising (see figure 1, column 3 lines 52-63 and column 10 lines 26 – column 11 line 40); a third computer (see figure 1 element 33 gateway node) on the network that screens the computer data from a first one of the first and second computers, wherein a result of the screening is communicated from the model to the second one of the first and second computers (column 10 lines 26 – column 11 line 40).

Ji does not teach a third computer on the network that comprises a model of a second one of the first and the second computers, the model configured to be

maintained and updated prior to receiving the computer data based on pre-existing information on the second computer to reflect any changes to the second one of the first and second computers.

Nachenberg teaches a third computer on the network that comprises a model of a second one of the first and the second computers, the model configured to be maintained and updated prior to receiving the computer data based on pre-existing information on the second computer to reflect any changes to the second one of the first and second computers and to screen the computer data from a first one of the first and second computers (see Nachenberg figure 4A and column 10 lines 12-57).

It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have install the computer data on a model machine to check of virus because it is the safest and most reliable way of check for viruses (see column 1 lines 34-46). Therefore one would have been motivated to have installed computer data on a model machine for the scanning of viruses.

With respect to claim 6, wherein the network comprises an IP network (see Ji column lines 17-32 i.e).

With respect to claim 8, wherein the network comprises a local area network (see figure 1 e.g. there is many element 30 in network 24), wherein the virus screening model resides outside the local area network (see figure 1 e.g. node 26).

With respect to claim 9, wherein the computer data comprises an electronic mail message (see Ji Abstract i.e. SMTP).

With respect to claim 10, wherein the computer data comprises data requested by the second computer from the first computer (see Ji Abstract, column 6 lines 55 – 61).

With respect to claim 14, wherein the model resides within a wide area network, and wherein the method further comprises: receiving across a local area network (see figure 1 element 22) a request for requested data from the first computer; sending the request across the wide area network to the second computer (see figure 1 e.g. element 30 in node 22 sends data to element 30 in network 26); and requesting that the requested data be returned via the model (see Ji figures 1, 6A, 6B, and 6C and column 6 lines 55 – column 9 line 26).

With respect to claim 15,receiving a request for the computer data from the first computer at a modem external to the first computer (see figure 1); and initiating communication of the computer data from the modem across an IP network to the second computer (see Ji column column 4 lines 17-32 i.e).

With respect to claim 19, wherein the network-based virus screening device resides within a wide area network, and wherein the method further comprises: configuring the model to inhibit communication of executables to the first computer (see Ji column 11 lines 6-40); and configuring an electronic mail system associated with the first computer to route messages addressed to the first computer through the model (see Ji figure 6A, 6B, 6C and column 6 lines 55 – 9 line 26).

With respect to claim 20, wherein the first computer is communicatively coupled to a local area network and the model resides outside a firewall associated with the

local area network, and wherein the method further comprises: configuring the network-based virus screening device to inhibit communication of executables to the first computer (see Ji column 11 lines 6-40); and configuring an electronic mail system associated with the first computer to route messages addressed to the first computer through the model (see Ji column 11 lines 6-40).

With respect to claim 21, wherein the screening result comprises a version of the computer data (column 10 lines 26 – column 11 line 40).

With respect to claim 22, further comprising using a reduced data version, simplified version, or modified version of the received computer data as the version of the computer data (column 10 lines 26 – column 11 line 40).

With respect to claim 23, further comprising generating a new installation program as the version of the received computer data (see Arnold column 8 line 28-60).

With respect to claim 24. (new) The method of claim 21, further comprising generating a handshake data packet as the version of the computer program (column 10 lines 26 – column 11 line 40).

With respect to claim 25. (new) The method of claim 1, wherein the screening comprises screening a portion of the computer data less than all of the computer data for the at least one virus (see Arnold column 8 line 28-60).

With respect to claim 28, wherein the maintaining and updating of the model comprises determining parameters of the second computer, wherein the parameters comprise a version of an operating system, a hardware type, registry information,

configuration information, or information from initialization files (see Arnold column 8 line 28-60).

With respect to claim 29, wherein the maintaining and updating of the model comprises requesting information from the second computer, obtaining information from the model if the information was created or altered by the installation program, and requesting information from a pre-existing image of the second computer (see Arnold column 8 line 28-60).

With respect to claim 30, wherein the pre-existing image of the second computer mimics a state of the second computer by maintaining a copy of settings and data stored to the second computer (see Arnold column 8 line 28-60).

With respect to claim 31, wherein the receiving, screening, and communicating of the computer data are performed unidirectionally or bidirectionally between the first and second computers (see Ji Abstract, column 3 lines 52-63 and column 10 lines 26 – column 11 line 40).

With respect to claim 32, wherein at least one of the first computer, the network, or the second computer is subscribed to a service providing the screening (see Ji Abstract, column 3 lines 52-63 and column 10 lines 26 – column 11 line 40).

With respect to claim 33, wherein the model determines from the screening result what is transmitted to the second computer (see Ji Abstract, column 3 lines 52-63 and column 10 lines 26 – column 11 line 40).

With respect to claim 34, wherein the second computer determines from the screening result what is transmitted to the second computer (see Ji Abstract, column 3 lines 52-63 and column 10 lines 26 – column 11 line 40).

With respect to claim 35, a computer-readable medium containing instructions for controlling at least one processor by a method comprising: receiving computer data (files) from a first computer (i.e. a node from which files came) at a intermediary of a second computer; screening the computer data for at least one virus using the model and producing a screening result; and communicating the screening result from the model to the second computer column 10 lines 26 – column 11 line 40 i.e. a recipient node which is to receive the files).

Ji does not teach wherein the intermediary computer is a model of the second computer and the model being maintained and updated to reflect any changes to the second one of the first and second computers. Nachenberg teaches wherein the intermediary computer is a model of the second computer (virtual machine) and maintained and updated the model prior to receiving the computer data based on pre-existing information on the second computer being to reflect any changes to the second one of the first and second computers (see Nachenberg figure 4A and column 10 lines 12-57).

It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have install the computer data on a model machine to check of virus because it is the safest and most reliable way of check for viruses (see column 1 lines 34-46). Therefore one would have

been motivated to have installed computer data on a model machine for the scanning of viruses.

With respect to claim 36, a system for transmitting computer data between a first computer and a second computer via a network, comprising: means for receiving the computer data (files) from a first computer (i.e. a node from which files came), means for screening the computer data for at least one virus; means for producing a screening result therefrom; and means for communicating the screening result to the second computer (column 10 lines 26 – column 11 line 40 i.e. a recipient node which is to receive the files).

Ji does not teach wherein the intermediary computer is a model of the second computer and the model being maintained and updated prior to receiving the computer data based on pre-existing information on the second computer prior to receiving the computer data based on pre-existing information on the second computer to reflect any changes to the second one of the first and second computers. Nachenberg teaches wherein the intermediary computer is a model of the second computer (virtual machine) and the model being maintained and updated to reflect any changes to the second one of the first and second computers (see Nachenberg figure 4A and column 10 lines 12-57).

It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have install the computer data on a model machine to check of virus because it is the safest and most reliable way of check for viruses (see column 1 lines 34-46). Therefore one would have

been motivated to have installed computer data on a model machine for the scanning of viruses.

With respect to claim 37, a system comprising: a processor; and a memory storing instructions that cause the processor to: receive computer data (files) from a first computer (i.e. a node from which files came) at a intermediary computer (see figure 1 element 33 gateway node) and communicate the screening result from the model to the second computer (see Ji Abstract, column 3 lines 52-63 and column 10 lines 26 – column 11 line 40).

Ji does not teach wherein the intermediary computer is a model of the second computer and the model being maintained and updated to reflect any changes to the second one of the first and second computers. Nachenberg teaches wherein the intermediary computer is a model of the second computer (virtual machine) and maintained and updated the model prior to receiving the computer data based on pre-existing information on the second computer being to reflect any changes to the second one of the first and second computers (see Nachenberg figure 4A and column 10 lines 12-57).

It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have install the computer data on a model machine to check of virus because it is the safest and most reliable way of check for viruses (see column 1 lines 34-46). Therefore one would have been motivated to have installed computer data on a model machine for the scanning of viruses.

With respect to claim 38, a method, comprising: causing a intermediary node to receive computer data from a first computer, the intermediary node being a model of a second computer; causing the intermediary node to be maintained and updated to reflect any changes to the second computer; causing the intermediary node (see figure 1 element 33 gateway node) to screen the computer data for at least one virus using the model and producing a screening result; and causing the intermediary node to communicate the screening result from to the second computer (see Ji Abstract, column 3 lines 52-63 and column 10 lines 26 – column 11 line 40).

Ji does not teach wherein the intermediary node is a model of the second computer and the model being maintained and updated to reflect any changes to the second one of the first and second computers. Nachenberg teaches wherein the intermediary computer is a model of the second computer (virtual machine) and maintained and updated the model prior to receiving the computer data based on pre-existing information on the second computer being to reflect any changes to the second one of the first and second computers (see Nachenberg figure 4A and column 10 lines 12-57).

It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have install the computer data on a model machine to check of virus because it is the safest and most reliable way of check for viruses (see column 1 lines 34-46). Therefore one would have been motivated to have installed computer data on a model machine for the scanning of viruses.

With respect to claim 39, a method comprising: maintaining a model of a destination computer (see figure 1 element 33 gateway node); analyzing data destined for the destination computer (i.e. receiving node) to determine whether the data includes a virus; and providing a screening result to the destination computer (see Ji Abstract, column 3 lines 52-63 and column 10 lines 26 – column 11 line 40).

Ji does not teach wherein the intermediary computer is a model of the second computer and receiving at a model of a second computer a status update communication from the second computer the status update communication including pre-existing information on the second computer; updating and maintaining the model based on the status update communication to reflect any changes to the second computer.

Nachenberg teaches wherein the intermediary computer is a model of the second computer (Virtual machine) and receiving at a model of a second computer a status update communication from the second computer the status update communication including pre-existing information on the second computer; updating and maintaining the model based on the status update communication to reflect any changes to the second computer (see Nachenberg figure 4A and column 10 lines 12-57).

It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have install the computer data on a model machine to check of virus because it is the safest and most reliable way of check for viruses (see column 1 lines 34-46). Therefore one would have

been motivated to have installed computer data on a model machine for the scanning of viruses.

Claim 27 is rejected under 35 U.S.C. 103(a) as being unpatentable over Ji et al (5,623,600) in view of Nachenberg (U.S. 5,696,822) in further view of Minkin et al (U.S. 6,826,698).

Ji and Arnold teah everything with respect to claim 1 above but with respect to claim 27 they do not teach switching between allowing and disallowing the screening based on enabling and disabling signals within the computer data. Minkin teaches switching between allowing and disallowing the screening based on enabling and disabling signals within the computer data (see column 1 lines 28-38). It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have to ability to turn off anti-virus based on the source of the data. Therefore one would have been motivated to have the ability to disable virus screening.

Allowable Subject Matter

Claims 26 is objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Devin Almeida whose telephone number is 571-270-1018. The examiner can normally be reached on Monday-Thursday from 7:30 A.M. to 5:00 P.M. The examiner can also be reached on alternate Fridays from 7:30 A.M. to 4:00 P.M.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron, can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/Devin Almeida/
Examiner, Art Unit 2432

/Gilberto Barron Jr./
Supervisory Patent Examiner, Art Unit 2432